FEDERAL

12 CFR Part 234

[Regulation HH; Docket No. R-1782]

RIN No. 7100-AG40

Financial Market Utilities

AGENCY: Board of Governors of the Federal Reserve System.

ACTION: Notice of Proposed Rulemaking.

SUMMARY: The Board of Governors of the Federal Reserve System (Board) is proposing to amend the requirements relating to operational risk management in the Board's Regulation HH, which applies to certain financial market utilities that have been designated as systemically important (designated FMUs) by the Financial Stability Oversight Council (FSOC) under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the Dodd-Frank Act or Act). The proposal would update, refine, and add specificity to the operational risk management requirements in Regulation HH to reflect changes in the operational risk, technology, and regulatory landscapes in which designated FMUs operate since the Board last amended this regulation in 2014. The proposal would also adopt specific incident-notification requirements.

DATES: Comments must be received by [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: You may submit comments, identified by Docket No. R-1782 and RIN 7100-AG40, by any of the following methods:

- **Agency Website:** http://www.federalreserve.gov. Follow the instructions for submitting comments at http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm.
- **E-mail:** regs.comments@federalreserve.gov. Include docket and RIN numbers in the subject line of the message.
- **FAX:** 202-452-3819 or 202-452-3102.

- **Mail:** Ann E. Misback, Secretary, Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue, NW, Washington, DC 20551.

Instructions: All public comments are available from the Board's website at http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm as submitted. Accordingly, comments will not be edited to remove any identifying or contact information. Public comments may also be viewed electronically or in paper in Room M-4365A, 2001 C Street, NW, Washington, DC 20551, between 9:00 a.m. and 5:00 p.m. during Federal business weekdays. For security reasons, the Board requires that visitors make an appointment to inspect comments. You may do so by calling (202) 452-3684. Upon arrival, visitors will be required to present valid government-issued photo identification and to submit to security screening in order to inspect and photocopy comments. For users of TTY-TRS, please call 711 from any telephone, anywhere in the United States.

FOR FURTHER INFORMATION CONTACT: Emily Caron, Assistant Director (202-452-5261) or Kathy Wang, Lead Financial Institution and Policy Analyst (202-872-4991), Division of Reserve Bank Operations and Payment Systems; or Cody Gaffney, Attorney (202-452-2674), Legal Division. For users of TTY-TRS, please call 711 from any telephone, anywhere in the United States.

SUPPLEMENTARY INFORMATION:

I. Background

A. Financial Market Utilities

A financial market utility (FMU) is a person that manages or operates a multilateral system for the purpose of transferring, clearing, or settling payments, securities, or other financial transactions among financial institutions or between financial institutions and the person.[1] FMUs provide essential infrastructure to clear and settle payments and other financial

[1] 12 U.S.C. 5462(6).

transactions. Financial institutions, including banking organizations, participate in FMUs pursuant to a common set of rules and procedures, technical infrastructure, and risk-management framework.

If a systemically important FMU fails to perform as expected or fails to effectively measure, monitor, and manage its risks, it could pose significant risk to its participants and the financial system more broadly. For example, the inability of an FMU to complete settlement on time could create credit or liquidity problems for its participants or other FMUs. An FMU, therefore, should have an appropriate and robust risk-management framework, including appropriate policies and procedures to measure, monitor, and manage the range of risks that arise in or are borne by the FMU.

B. Title VIII of the Dodd-Frank Act

In recognition of the criticality of FMUs to the stability of the financial system, Title VIII of the Dodd-Frank Act (the Dodd-Frank Act or Act) established a framework for enhanced supervision of certain FMUs. Section 804 of the Dodd-Frank Act states that the FSOC shall designate those FMUs that it determines are, or are likely to become, systemically important. Such a designation by the FSOC makes an FMU subject to the supervisory framework set out in Title VIII of the Act.

Section 805(a)(1)(A) of the Act requires the Board to prescribe risk-management standards governing the operations related to payment, clearing, and settlement activities of designated FMUs.[2] As set out in section 805(b) of the Act, the applicable risk-management

---

[2] 12 U.S.C. 5464(a)(1). The Act directs the Board to "tak[e] into consideration relevant international standards and existing prudential requirements" when it promulgates these risk-management standards. *Id.* In addition, section 805(a)(2) of the Act grants the U.S. Commodity Futures Trading Commission (CFTC) and the U.S. Securities and Exchange Commission (SEC) the authority to prescribe such risk-management standards for a designated FMU that is, respectively, a derivatives clearing organization (DCO) registered under section 5b of the Commodity Exchange Act, or a clearing agency registered under section 17A of the Securities Exchange Act of 1934. 12 U.S.C. 5464(a)(2).

standards must (1) promote robust risk management, (2) promote safety and soundness, (3) reduce systemic risks, and (4) support the stability of the broader financial system.[3]

A designated FMU is subject to examination by the federal agency that has primary jurisdiction over the FMU under federal banking, securities, or commodity futures laws (the "Supervisory Agency").[4] At present, the FSOC has designated eight FMUs as systemically important, and the Board is the Supervisory Agency for two of these designated FMUs – The Clearing House Payments Company, L.L.C. (on the basis of its role as operator of the Clearing House Interbank Payments System (CHIPS)) and CLS Bank International.[5] The risk-management standards in the Board's Regulation HH apply to Board-supervised designated FMUs.[6]

C. Regulation HH Risk-Management Standards for Designated FMUs

Section 234.3 of Regulation HH includes a set of 23 risk-management standards addressing governance, transparency, and the various risks that can arise in connection with a designated FMU's payment, clearing, and settlement activities, including legal, financial, and operational risks. These standards are based on and generally consistent with the *Principles for*

---

[3] Further, under section 805(c), the risk-management standards may address areas such as (1) risk-management policies and procedures, (2) margin and collateral requirements, (3) participant or counterparty default policies, (4) the ability to complete timely clearing and settlement of financial transactions, (5) capital and financial resource requirements for designated FMUs, and (6) other areas that are necessary to achieve the objectives and principles described above. 12 U.S.C. 5464(c).

[4] The Act's definition of "Supervisory Agency" is codified at 12 U.S.C. 5462(8). Section 807 of the Act authorizes the Supervisory Agencies to examine and take enforcement actions against the Supervisory Agencies' respective designated FMUs. The Act also describes certain authorities that the Board has with respect to designated FMUs for which it is not the Supervisory Agency, such as participation in examinations and recommendations on enforcement actions. 12 U.S.C. 5466.

[5] The SEC is the Supervisory Agency for The Depository Trust Company (DTC); Fixed Income Clearing Corporation (FICC); National Securities Clearing Corporation (NSCC); and The Options Clearing Corporation (OCC). The CFTC is the Supervisory Agency for the Chicago Mercantile Exchange, Inc. (CME); and ICE Clear Credit LLC (ICC). *See* U.S. Department of the Treasury, *Financial Market Utility Designations*, https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc/designations.

[6] The risk-management standards in Regulation HH would also apply to any designated FMU for which another Federal banking agency is the Supervisory Agency. At this time, there are no such designated FMUs.

Financial Market Infrastructures (PFMI).[7] The Regulation HH standards generally employ a flexible, principles-based approach. In several cases, however, the Board adopted specific minimum requirements that a designated FMU must meet in order to achieve the overall objective of a particular standard.

1. Operational risk management

Section 234.3(a)(17) of Regulation HH requires that a designated FMU manage its operational risks by establishing a robust operational risk-management framework that is approved by its board of directors.[8] In this regard, the designated FMU must (1) identify and mitigate its plausible sources of operational risk; (2) identify, monitor, and manage the operational risks it may pose to other FMUs and trade repositories; (3) ensure a high degree of security and operational reliability; (4) have adequate, scalable capacity to handle increasing stress volumes; (5) address potential and evolving vulnerabilities and threats; and (6) provide for rapid recovery and timely resumption of critical operations and fulfillment of obligations, including in the event of a wide-scale or major disruption. Section 234.3(a)(17) also contains several specific minimum requirements for business continuity planning, including a requirement for the designated FMU to have a business continuity plan that (1) incorporates the use of a secondary site at a location with a distinct risk profile from the primary site; (2) is designed to enable critical systems to recover and resume operations no later than two hours following disruptive events; (3) is designed to enable it to complete settlement by the end of the day of the disruption, even in case of extreme circumstances; and (4) is tested at least annually.

Although the term "operational risk" is not defined in current Regulation HH, when the Board proposed amendments to § 234.3(a)(17) in 2014, it described operational risk as the risk

---

[7] The PFMI, published by the Committee on Payment and Settlement Systems (now the Committee on Payments and Market Infrastructures) and the Technical Committee of the International Organization of Securities Commissions in April 2012, is widely recognized as the most relevant set of international risk-management standards for payment, clearing, and settlement systems.

[8] In this notice, § 234.4(a)(17) will be informally referred to as the "operational risk management standard."

that deficiencies in information systems, internal processes, and personnel or disruptions from external events will result in the deterioration or breakdown of services provided by an FMU.[9] Consistent with an all-hazards view of managing operational risk, the Board believes operational risk could arise internally and externally. Internal sources of operational risk include the designated FMU's people, processes, and technology.[10] External sources of operational risk are those that fall outside the direct control of a designated FMU. For example, external sources of operational risk can include the designated FMU's participants and other entities, such as other FMUs, settlement banks, liquidity providers, and service providers, which may transmit threats through their various connections to the designated FMU. External sources of operational risk also include physical events, such as pandemics, natural disasters, and other destruction of property, as well as information security threats, such as cyberattacks and technology supply chain vulnerabilities. These internal and external sources of operational risk can manifest in different scenarios (including wide-scale or major disruptions) and can result in the reduction, deterioration, or breakdown of services that a designated FMU provides. A designated FMU must plan for these types of scenarios and test its systems, polices, procedures, and controls against them.

Importantly, the Board believes that effective operational risk-management, in combination with sound governance arrangements and effective management of general business risk (including the risk of losses from operational events), promotes operational resilience, which refers to the ability of an FMU to: (1) maintain essential operational capabilities under adverse conditions or stress, even if in a degraded or debilitated state; and (2) recover to effective

---

[9] 79 FR 3665, 3683 (Jan. 22, 2014). The Board also incorporated this definition of "operational risk" into part I of the *Federal Reserve Policy on Payment System Risk* (PSR policy) in 2014, *see* 79 FR 2838, 2845 (Jan. 16, 2014), and into its ORSOM rating system in 2016, *see* 81 FR 58932, 58936 (Aug. 26, 2016). The PSR policy is available at https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf.

[10] Deficiencies in assessing and managing these sources of operational risk could cause errors or delays in processing, systems outages, insufficient capacity, fraud, data loss, and data leakage.

operational capability in a time frame consistent with the provision of critical economic services.[11]

2. Evolution in the operational risk, technology, and regulatory landscape

When the Board proposed the current Regulation HH risk-management standards in 2014, it recognized that there was ongoing work and discussion domestically and internationally on developing operational risk-management standards and planning for business continuity with respect to cybersecurity and responses to cyberattacks.[12] For example, in 2016, the Committee on Payments and Market Infrastructures (CPMI) and Technical Committee of the International Organization of Securities Commissions (IOSCO) published *Guidance on cyber resilience for financial market infrastructures* (Cyber Guidance), which supplements the PFMI and provides guidance on cyber resilience, including in the context of governance, the comprehensive management of risks, and operational risk management.[13] The Cyber Guidance has informed the Federal Reserve's supervision of designated FMUs.[14]

More recently, new challenges to operational risk management have emerged, including a global pandemic and severe weather events. In addition, certain types of cyberattacks that were once thought to be extreme or "tail-risk" events, like attacks on the supply chain and ransomware attacks, have become more prevalent. Technology solutions for the management of operational risk have also advanced since 2014, including the development of new technologies that have the potential to improve the resilience of designated FMUs. Finally, the legal and regulatory landscape in which designated FMUs operate has evolved to reflect these changes in the broader operational risk environment. For example, in November 2021, the Board, the Office of the

---

[11] *See* § 234.3(a)(2) and (a)(15).

[12] 79 FR 3665, 3683 (Jan. 22, 2014)

[13] CPMI-IOSCO, *Guidance on Cyber Resilience for Financial Market Infrastructures* (June 2016), https://www.bis.org/cpmi/publ/d146.htm.

[14] For example, when the Board finalized its ORSOM rating system for designated FMUs in 2016, it noted that the then-forthcoming Cyber Guidance would guide the Board's assessment of a designated FMU with respect to operational risk and cybersecurity policies and procedures. 81 FR 58932, 58934 (Aug. 26, 2016).

Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) adopted requirements on computer-security incident notifications for banking organizations and bank service providers (interagency notification rule).[15]

The evolution in the operational risk, technology, and regulatory landscape motivated the Board to conduct a full review of § 234.3(a)(17) to determine whether updates are necessary. Following this review, the Board believes that the outcomes required by the current operational risk management standard are generally still relevant and comprehensive. However, the Board has identified several areas where it believes updates to the rule are necessary.

II. Explanation of Proposed Rule

The Board is proposing to amend its operational risk management standard to reflect changes in the operational risk and threat landscape, as well as to incorporate developments in designated FMUs' operations and technology usage since the Board last amended Regulation HH in 2014. The proposal focuses on four areas: (1) review and testing, (2) incident management and notification, (3) business continuity management and planning, and (4) third-party risk management. The Board is also proposing several technical or clarifying amendments throughout §§ 234.2 and 234.3(a).[16]

The Board believes that the proposal continues to employ a flexible, principles-based approach in Regulation HH. Further, the Board believes the proposed amendments are largely consistent with existing measures that designated FMUs take to comply with Regulation HH and would create minimal added burden for the designated FMUs that are subject to Regulation HH.

---

[15] 86 FR 66424 (Nov. 23, 2021). Congress also recently enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022, which requires covered entities to report significant cyber incidents to the Cybersecurity and Infrastructure Agency ("CISA"). *See* H.R. 2471, 117th Cong. (2022).

[16] In addition to the technical changes described below in section II.E, the Board is also proposing a technical change to the title of § 234.3. Currently, the section is erroneously titled "Standards for payment systems," which is the legacy title from the initial Regulation HH risk-management standards published in 2012. The Board is proposing to replace "payment systems" with "designated financial market utilities."

Accordingly, the Board is proposing that the proposed changes would become effective and require compliance 60 days from the date a final rule is published in the *Federal Register*.

The Board requests comment on all aspects of the proposed amendments, including the proposed effective and compliance date. In addition, the Board requests comment on the specific questions below. Where possible, commenters should provide both quantitative data and detailed analysis in their comments, particularly with respect to suggested alternatives to the proposed amendments. Commenters should also explain the rationale for their suggestions.

A. Review and Testing

Currently, § 234.3(a)(17)(i) requires designated FMUs to identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls that are reviewed, audited, and tested periodically and after major changes. This general review and testing requirement applies broadly to the systems, policies, procedures, and controls that the designated FMU develops to mitigate sources of operational risk. For example, designated FMUs need to design and conduct appropriate tests on any policies or systems that they develop to ensure a high degree of security and operational reliability (as required by § 234.3(a)(17)(iii)). Similarly, a designated FMU needs to review and test any arrangements it sets up to achieve its planned business continuity recovery and resumption objectives (as required by § 234.3(a)(17)(vii)). This general review and testing requirement encompasses all reviews and tests the designated FMU performs with respect to such systems, policies, procedures, and controls, including those performed by the designated FMU's business lines, risk-management function, and audit function. It does not, however, prescribe specific types of tests that the designated FMU must conduct.

The Board is proposing amendments to the general review and testing requirement that would provide more specificity regarding its expectations. Proposed § 234.3(a)(17)(i) would emphasize that, just as the current general review and testing requirement applies broadly to the designated FMU's systems, policies, procedures, and controls, the proposal's requirements

would also apply broadly to the systems, policies, procedures, and controls developed to mitigate the impact of the designated FMU's sources of operational risk.

1. Testing

Proposed § 234.3(a)(17)(i)(A)(1) would require a designated FMU to conduct tests of its systems, policies, procedures, and controls in accordance with a documented testing framework. The documented testing framework would need to address, at a minimum, the scope and frequency of such testing, who participates in such testing, and how the results of such testing will be reported. The testing framework would also need to account for any interdependencies between and among the systems, policies, procedures, and controls that are being tested.[17] A designated FMU could describe its testing framework in either a single document or in multiple documents, as appropriate, and could leverage relevant industry standards as it develops its testing framework.[18]

Proposed § 234.3(a)(17)(i)(A)(2) would require that the tests that a designated FMU conducts assess whether its systems, policies, procedures, or controls function as intended. Such tests could include capacity stress tests, crisis management tabletop exercises, after-action reviews of incidents, business continuity tests both internally and with participants, vulnerability assessments, cyber scenario-based testing, penetration tests, and red team tests. Importantly, as described further below, a designated FMU would need to remediate any deficiencies identified during testing.

2. Review scope

Proposed § 234.3(a)(17)(i)(B) would require a designated FMU to conduct a review of the design, implementation, and testing of relevant systems, policies, procedures, and controls

---

[17] The proposal emphasizes the need for a designated FMU to take a comprehensive and risk-based approach to its operational risk management testing program, rather than focusing only on testing individual (or groups of) systems, policies, procedures, or controls (or components therein).

[18] For example, a designated FMU could leverage standards developed by the National Institute of Standards and Technology (NIST) and the Federal Financial Institutions Examination Council (FFIEC).

after the designated FMU experiences any material operational incidents (which are discussed in section II.B.2 below). A designated FMU would also need to conduct such a review after significant changes to the environment in which it operates.[19]

The operational risk environment, including sources of risk and the nature or types of threats, can change unexpectedly and quickly. The proposal would ensure that designated FMUs review and make timely changes to their systems, policies, procedures, and controls following such changes. For example, the COVID-19 global pandemic highlighted new risks and challenges in the operational risk environment that warrant a review of relevant systems, policies, procedures, and controls.

3. Remediation of identified deficiencies

Finally, proposed § 234.3(a)(17)(i)(C) would require a designated FMU to remediate as soon as possible, following established governance processes, any deficiencies identified during tests and reviews. A designated FMU would need to assess whether such identified deficiencies require urgent remediation or are less urgent. In order to ensure that remediation measures are effective, it would be imperative for a designated FMU to perform subsequent validation to assess whether the remediation measures have addressed deficiencies without introducing new vulnerabilities.

A designated FMU should consult widely used and relevant industry standards to inform its understanding of how it should remediate any deficiencies. These industry standards, such as those published by the National Institute of Standards and Technology (NIST), the Federal Financial Institutions Examination Council (FFIEC), the Financial Services Sector Coordinating Council (FSSCC), and the International Organization for Standardization (ISO), are updated

[19] The Board is also proposing a technical amendment to the requirement for the designated FMU to *review* its recovery and orderly wind-down plan under § 234.3(a)(3)(iii)(G) from "following" to "after" changes to the designated FMU's systems and environment. This conforms with the review requirement under proposed § 234.3(a)(17)(i)(B). The Board is also proposing a technical amendment to the requirement for the designated FMU to *update* its public disclosure under § 234.3(a)(23)(v) from "following" to "to reflect" changes to its systems and environment.

regularly and typically offer current and specific information on operational risk management practices.

4. Questions

With respect to proposed § 234.3(a)(17)(i)(A)-(C), the Board requests comment on the following specific questions:

1. Are the elements listed in § 234.3(a)(17)(i)(A)(1) the right elements to include by rule in the testing framework? What other elements should be addressed in a rule for a testing framework?
2. Are there challenges associated with implementation of these proposed requirements that the Board has not considered?

B. Incident Management and Notification

The Board is proposing to establish incident management and notification requirements in proposed § 234.3(a)(17)(vi).

1. Documented incident management framework

Proposed § 234.3(a)(17)(vi) would require a designated FMU to establish a documented framework for incident management that provides for the prompt detection, analysis, and escalation of an incident; appropriate procedures for addressing an incident; and incorporation of lessons learned following an incident.[20]

In line with the all-hazards approach to operational risk management in this standard, the Board believes it is important for a designated FMU to be prepared to detect, address, and learn from any type of operational incident, regardless of the scenario or source of risk and the level of severity. Different types of incidents may require different levels of escalation internally or externally. Different types of incidents may also require different strategies for containment or

[20] These broad categories in incident management are generally consistent with those identified in the NIST computer-security incident handling guide. *See* NIST, *Computer Security Incident Handling Guide* (Special Publication 800-61, rev. 2), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

eradication. For example, given the increasing prevalence of cyberattacks in the financial sector, a designated FMU should plan for an incident where a participant (or another type of connected entity), rather than the designated FMU itself, is experiencing a cyberattack. In this scenario, a designated FMU should be operationally prepared to take, and should have a legal basis to take, appropriate steps to mitigate the risk of contagion to itself or other participants, including but not limited to disconnecting the participant from the FMU if necessary. A designated FMU should also have processes and procedures to determine whether and when it would be appropriate to allow such a participant to reconnect to the FMU.

The proposal would require that a designated FMU's incident management framework include a plan for notification and communication of material operational incidents. This plan would, among other things, need to identify the entities that would be notified of operational incidents, including non-participants that could be affected by material operational incidents at the designated FMU and appropriate industry information-sharing fora. Proposed § 234.3(a)(17)(vi)(A) and (B), which are discussed further in sections II.B.2 and II.B.3, would set forth more detailed requirements for notification and communication of material incidents to ensure that the Board, the designated FMU's participants, and other relevant entities receive timely notifications.

2. Incident notification to the Board

Proposed § 234.3(a)(17)(vi)(A) would require a designated FMU to notify the Board of operational incidents.

In November 2021, the Board, FDIC, and OCC jointly adopted the interagency notification rule for banking organizations and bank service providers.[21] The interagency notification rule scoped out designated FMUs, but the preamble to the interagency rule explained that the Board believes it is important for designated FMUs to inform Federal Reserve

[21] 86 FR 66424 (Nov. 23, 2021).

supervisors of operational disruptions on a timely basis.[22] The preamble to the interagency rule also noted that the Board would consider proposing amendments to Regulation HH in the future to formalize its incident-notification expectations and promote consistency between requirements applicable to designated FMUs that are supervised by the Board, the U.S. Securities and Exchange Commission (SEC), and the U.S. Commodity Futures Trading Commission (CFTC).[23]

Under proposed § 234.3(a)(17)(vi)(A), a designated FMU would be required to immediately notify the Board when it activates its business continuity plan or has a reasonable basis to conclude that (1) there is an actual or likely disruption, or material degradation, to any of its critical operations or services,[24] or to its ability to fulfill its obligations on time; or (2) there is unauthorized entry, or the potential for unauthorized entry, into the designated FMU's computer, network, electronic, technical, automated, or similar systems that affects or has the potential to affect its critical operations or services. Given the large volume and value of payment, clearing, and settlement activity processed by these entities and their interconnectedness with financial institutions and markets, material operational issues occurring at these designated FMUs could have financial stability implications. It is therefore critical for the Board to be notified immediately of these types of issues.

Importantly, in addition to actual disruptions, material degradation, or unauthorized entries, the proposal would also require immediate notification to the Board if the designated FMU has a reasonable basis to conclude that a disruption or material degradation is "likely" to occur or if there is "potential" for unauthorized entry into the designated FMU's computer,

---

[22] *Id*. at 66428 (noting that "the Board has generally observed such practice by designated FMUs").

[23] *Id.* SEC-supervised designated FMUs are subject to the SEC's Regulation SCI, which generally requires covered entities to notify the SEC "immediately" and their members or participants "promptly" of an SCI event. *See* 17 CFR 242.1000 (defining "SCI Event") and 242.1002 (imposing notification requirements related to SCI Events). Similarly, a CFTC-supervised designated FMU must notify the CFTC "promptly" of an "exceptional event". *See* 17 CFR 39.18(g). An "exceptional event" includes "[a]ny hardware or software malfunction, security incident, or targeted threat that materially impairs, or creates a significant likelihood of material impairment, of automated system operation, reliability, security, or capacity; or [a]ny activation of the designated FMU's business continuity and disaster recovery plan." *Id.*

[24] Critical operations and critical services are discussed below in section II.E.2.

network, electronic, technical, automated, or similar systems that affects or has the potential to affect its critical operations or services. For example, a hurricane in the region where the designated FMU is located would not alone trigger notification; however, if the designated FMU concludes that such an event likely would disrupt or materially degrade its critical operations or services, then notification would be required. Similarly, in the case of potential unauthorized entries, not all identified vulnerabilities in its systems would require an immediate notification. However, if a designated FMU discovers or becomes aware of an unexploited vulnerability and determines that, if exploited, such vulnerability could result in a disruption or material degradation of its critical operations or service, the designated FMU would need to notify the Board immediately of such discovery.

The Board notes that "immediately" is meant to convey the urgency in notifying the Board of these material operational incidents; it does not mean "instantaneous" notification. The Board would expect to be notified of an operational incident once the designated FMU activates its business continuity plan or has a reasonable basis to conclude that an incident meets any of the criteria in proposed § 234.3(a)(17)(vi)(A)(1)-(2), even if the designated FMU does not yet have detailed information on the root cause or measures for containment or remediation. In these cases, the Board would expect to receive any available information that the designated FMU has at the time of notification.

The Board recognizes that the requirement for "immediate" notification to the Board would establish a heightened requirement for designated FMUs relative to banking organizations.[25] The proposed requirement is consistent with the systemic importance of designated FMUs and with existing SEC and CFTC incident notification requirements for the designated FMUs for which either the SEC or the CFTC is the Supervisory Agency.

---

[25] Under the interagency notification rule, a banking organization must notify its primary Federal regulator of certain computer-security incidents "as soon as possible and no later than 36 hours." *See* 86 FR 66424, 66431–32 (discussing timing of notification to agencies).

3. Incident notification to participants and other relevant entities

Proposed § 234.3(a)(17)(vi)(B) would require a designated FMU to establish criteria and processes, including the appropriate methods of communication, to provide for timely communication and responsible disclosure of material operational incidents to its participants or other relevant entities that have been identified in its notification and communication plan.

As proposed, this incident notification requirement would arise in two circumstances. First, a designated FMU would need to notify affected participants immediately in the event of actual disruptions or material degradation to its critical operations or services or to its ability to fulfill its obligations on time.[26] This immediate notification would ensure that affected participants (e.g., participants encountering delays or errors) are aware that the issue originates from the designated FMU and not their own systems, in order to minimize confusion in the markets that the designated FMU serves and to allow participants to assess the impact to their operations. The term "immediately" is meant to convey the urgency in notifying the designated FMU's participants of disruptions or material degradation to its services; it does not mean "instantaneous" notification.

Second, a designated FMU would need to notify all participants and other relevant entities[27] in a timely and responsible manner of all other material operational incidents that require immediate notification to the Board. When designing this part of its communication plan, the Board would expect a designated FMU to consider the timing, content, recipients, and method of notification for a range of potential material operational incidents. In determining the scope of disclosure for a particular incident, the Board would expect a designated FMU to consider factors such as the risk-mitigation benefits arising from early warning to the financial

---

[26] The requirement for "immediate" notification to affected participants would establish a heightened requirement for designated FMUs relative to those imposed on bank service providers in the interagency rule (which requires notification "as soon as possible"), consistent the systemic importance of designated FMUs.

[27] As described in section II.B.1, above, a designated FMU would need to identify non-participant relevant entities in its plan for notification and communication of material operational incidents.

system, the safety and soundness of the designated FMU, and any financial stability implications of disclosure. The Board recognizes that there might be risks to providing early disclosures to a broad audience regarding certain types of material operational issues. For example, if a designated FMU identifies a cyber vulnerability, the designated FMU might weigh the risk of disclosure as sufficiently great to delay notification or tailor the information provided to avoid exposing the designated FMU to a cyberattack.

4. Examples of material operational incidents

The following is a non-exhaustive list of operational incidents that the Board would consider to be material for purposes of the proposal. The Board would expect examples 1 and 2 to trigger immediate notifications to the Board and to the designated FMU's participants (and notification in a timely manner to other relevant entities, as applicable). The Board would expect examples 3–5 to trigger immediate notification to the Board, but believes the designated FMU should determine when they may trigger appropriately timely notifications and disclosure to participants and non-participant entities based on the criteria in its notification and communication plan.

1) Large-scale distributed denial of service attacks that prevent the designated FMU from receiving its participants' payment instructions.
2) A severe weather event or other natural disaster that causes significant damage to a designated FMU's production site and necessitates failover to another site during the business day.
3) Malware on a designated FMU's network that poses an imminent threat to its critical operations or services (such as its core payment, clearing, or settlement processes, or collateral management processes), or that may require the designated FMU to disengage any compromised products or information systems that support the designated FMU's critical operations and services from internet-based network connections.

4) A ransom malware attack that encrypts a critical system or backup data.

5) A zero-day vulnerability on software that the designated FMU uses and has determined, if exploited, could lead to a disruption to or material degradation of its critical operations or services.

5. Questions

With respect to proposed § 234.3(a)(17)(vi), the Board requests comment on the following specific questions:

3. Do the requirements under proposed § 234.3(a)(17)(vi)(A) strike the proper balance between providing the Board with early warning and allowing designated FMUs sufficient time to notify the Board?
4. How should the criteria for determining whether operational incidents are material enough to warrant notification to the Board under proposed § 234.3(a)(17)(vi)(A) be modified, if at all?
5. Should the Board provide additional examples of material operational incidents?
6. How should designated FMUs provide notifications to the Board? For example, should the Board establish a centralized point of contact to receive notifications, or should designated FMUs notify their supervisory teams?
7. Is the proposed requirement on planning for timely notification and "responsible disclosure" of material operational incidents clear? Should a term other than "responsible" disclosure be used, given the intention of this proposed requirement, as explained in section II.B.3 above?
8. Are there challenges associated with implementing these proposed requirements that the Board has not considered?

C. Business Continuity Management and Planning

Current § 234.3(a)(17)(vi) (which, under the proposal, would be renumbered as § 234.3(a)(17)(vii)) requires that a designated FMU have business continuity management that

provides for rapid recovery and timely resumption of its critical operations and fulfillment of its obligations, including in the event of a wide-scale or major disruption. Current § 234.3(a)(17)(vii) (which, under the proposal, would be renumbered as § 234.3(a)(17)(viii)) elaborates on certain requirements for a designated FMU's business continuity plan. Specifically, a business continuity plan must incorporate the use of a secondary site with a distinct risk profile from the primary site; be designed to enable critical systems to recover and resume operations no later than two hours following disruptive events; be designed to complete settlement by the end of the day of the disruption, even in extreme circumstances; and be tested at least annually.

The proposed amendments to current § 234.3(a)(17)(vii) would provide further detail in Regulation HH related to business continuity management and planning in order to promote robust risk management, reduce systemic risks, increase safety and soundness, and support the stability of the broader financial system.

1. Two sites providing for sufficient redundancy

The proposal would amend current § 234.3(a)(17)(vii)(A) to update terminology related to required backup sites. Currently, § 234.3(a)(17)(vii)(A) requires a designated FMU to have a secondary site that is located at a sufficient geographical distance from the primary site to have a distinct risk profile. The Board proposes to replace the references to "secondary site" and "primary site" with a general reference to "two sites providing for sufficient redundancy supporting critical operations and services" that are located at a sufficient geographical distance from "each other" to have a distinct risk profile (collectively, "two sites with distinct risk profiles").

This proposed amendment would accommodate data center arrangements with multiple production sites, rather than reflecting only the traditional arrangement where one site is considered "primary" and another site is treated distinctly as a backup site. The proposal would still require, however, a minimum of two locations that are sufficiently geographically distant from each other to have a distinct risk profile. Consistent with the Board's explanation when it

adopted the current text of Regulation HH in 2014, the Board would consider sites to have "distinct risk profiles" if, for example, they are not located in areas that would be susceptible to the same severe weather event (e.g., the same hurricane zone) or on the same earthquake fault line. These sites would likely also have distinct power and telecom providers and be operated by geographically dispersed staff.

2. Recovery and resumption

Current § 234.3(a)(17)(vi) establishes a broad requirement for business continuity management. Current § 234.3(a)(17)(vii)(B)-(C) sets specific recovery and resumption objectives, requiring that a designated FMU's business continuity plan be designed to enable, respectively, recovery and resumption no later than two hours following disruptive events and completion of settlement by the end of the day of the disruption, even in case of extreme circumstances.

Under the proposal, these requirements would remain substantively unchanged.[28] Since the Board established these requirements in Regulation HH, the two-hour recovery time objective has been a particular area of focus during bilateral discussions with Board-supervised designated FMUs, as well as in broader domestic and international fora, specifically in the context of extreme cyber events. At the center of those discussions is the balance between timely recovery and resumption of critical operations and appropriate assurance that critical operations are restored to a trusted state. The Board continues to believe it is imperative to financial stability that a designated FMU be able to recover and resume its critical operations and services quickly after disruptive events, physical and cyber, and to complete settlement by the end of the day of the disruption. In related discussions with Board-supervised firms, and supported by provisions in the CPMI-IOSCO Cyber Guidance, Board staff has emphasized that recovery time objectives

[28] In addition to renumbering these sections as § 234.3(a)(17)(vii) and § 234.3(a)(17)(viii)(B)-(C), respectively, the Board is proposing a technical revision to § 234.3(a)(17)(vi), as described below in section II.E.2.

are necessary and critical targets around which plans, systems, and processes should be designed, enabling the firm to meet the objective.[29] However, these recovery time objectives should not be interpreted as a requirement for a designated FMU to resume operations in a compromised or otherwise untrusted state.

Threats to designated FMUs' operations continue to evolve, and the Board expects that a designated FMU's business continuity planning will be a dynamic process in which the designated FMU works to update the scenarios for which it plans on an ongoing basis to meet its recovery and resumption objectives. For many types of disruptive scenarios, technology and methods already exist to enable a designated FMU to recover and resume operations within two hours of the disruption. For example, if an earthquake damages a designated FMU's hardware and disrupts operations at one data center, the designated FMU can fail over to another location that is outside the earthquake radius.

The Board recognizes, however, that certain threats to designated FMUs' operations, as well as the technology to mitigate those threats, are continually evolving. In areas where threats and technology are still evolving, such as is the case for extreme cyberattacks (e.g., where significant data loss or corruption occurs across its data centers), the Board recognizes that solutions are evolving with the threat environment and require a holistic approach that integrates protective, detective, and containment measures with response, recovery, and resumption solutions. The Board continues to expect that a designated FMU's business continuity planning will be a dynamic process in which the designated FMU works on an ongoing basis to update its plan to recover and resume operations to achieve its objectives in light of these evolving threats.

---

[29] For example, paragraph 6.2.2 of the Cyber Guidance notes that the objectives for resuming operations set goals for, ultimately, the sound functioning of the financial system, which should be planned for and tested against. It further notes the criticality of the recovery and resumption objectives under Principle 17, Key Consideration 6 of the PFMI, while also acknowledging that financial market infrastructures should exercise judgment in effecting resumption so that risks to itself or its ecosystem do not thereby escalate. For additional details, *see* CPMI-IOSCO, *Guidance on Cyber Resilience for Financial Market Infrastructures* (June 2016) at section 6, https://www.bis.org/cpmi/publ/d146.htm ("Response and Recovery").

Federal Reserve supervisors will also continue to work with designated FMUs through the supervisory process as designated FMUs identify reasonable approaches to prepare for and recover from such attacks. As development of adequate solutions for extreme cyberattacks continues, designated FMUs should also plan for contingency scenarios in which planned recovery and resumption objectives cannot be achieved. Planning for such scenarios would also be in accordance with national policies aimed at improving the cybersecurity posture of U.S. critical infrastructures.[30]

3. Reconnection after a disruption to the designated FMU's critical operations or services

Proposed § 234.3(a)(17)(viii)(D) would require that the business continuity plan set out criteria and processes that address the reconnection of a designated FMU to its participants and other entities following a disruption to the designated FMU's critical operations or services. In this context, the Board would consider a disruption to a designated FMU's critical operations or services broadly as a form of "disconnection" to external parties such as the designated FMU's participants. This would include situations where a designated FMU deliberately takes itself offline such that participants cannot access its services (e.g., if it experiences a major cyberattack that it needs to contain); it would also include situations where a designated FMU loses connection to its participants due to another type of external event (e.g., if its production site loses power due to a severe weather event in its region).

The Board believes that the current requirements to plan for recovery and resumption include an implicit expectation that a designated FMU plan to reconnect to its participants and other relevant entities following a disruption. However, the Board is proposing to make this expectation explicit in order to emphasize the importance of *ex ante* criteria and processes addressing when and how a designated FMU will reconnect to its participants and other relevant

---

[30] *See, e.g.*, Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience* (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

entities. Given the current threat landscape and the ability for malware to spread, the Board believes it is crucial for a designated FMU to be prepared to balance the need for the designated FMU to quickly recover and resume its critical operations against the risk of contagion to its ecosystem should it resume operations in an unsafe state (e.g., before an extremely harmful computer virus is fully contained or eradicated). For cyber incidents, it is particularly important for a designated FMU to be prepared to assure its participants, other connected entities, and regulator(s) that its remediation efforts are complete and that it has achieved a safe and trusted state.[31] A designated FMU should consider establishing a phased approach to reconnecting to the designated FMU's participants and other relevant entities, transaction testing with selected participants before full reconnection, and heightened monitoring for an appropriate period of time after reconnection.

4. Business continuity testing

The proposal would amend current § 234.3(a)(17)(vii)(D), which requires the business continuity plan to be "tested at least annually," by separating it into two requirements (proposed § 234.3(a)(17)(viii)(E) and (F)).

Proposed § 234.3(a)(17)(viii)(E) would maintain the requirement for at least annual testing and clarify that this requirement covers the designated FMU's business continuity arrangements, including the people, processes, and technologies of the two sites with distinct risk profiles.[32] The required testing would need to demonstrate that the designated FMU is able to run live production at the two sites with distinct risk profiles; that its solutions for data recovery and data reconciliation enable it to meet its objectives to recover and resume operations two hours following a disruption and enable settlement by the end of the day of the disruption even in case of extreme circumstances including if there is data loss or corruption; and that it has

[31] A designated FMU might consider leveraging third-party experts to verify its remediation efforts.

[32] These tests would be subject to the general testing requirements described in section II.A.1 above.

geographically dispersed staff who can effectively run the operations and manage the business of the designated FMU.

The Board believes that a designated FMU must be able to demonstrate these particular capabilities in order verify that its business continuity arrangements will function as intended in achieving the recovery and resumption objectives in its business continuity plan. For example, given the importance of developing effective solutions for data recovery and reconciliation to address extreme cyber scenarios, the Board believes that designated FMUs should expressly be required to demonstrate that such solutions function as intended. Designated FMUs should also continue to plan for and test other scenarios, including wide-scale disruptions and major disruptions, from which they may need to recover.[33]

Proposed § 234.3(a)(17)(viii)(F) would require a designated FMU to review its business continuity plans, pursuant to the general review requirements described in section II.A.2 above, at least annually. The objectives of this review are twofold: (1) to incorporate lessons learned from actual and averted disruptions, and (2) to update the scenarios considered and assumptions built into the plan in order to ensure responsiveness to the evolving risk environment and incorporate new and evolving sources of operational risk (e.g., extreme cyber events).

5. Questions

With respect to proposed § 234.3(a)(17)(viii), the Board requests comment on the following specific questions:

9. What are reasonable estimates of the costs and other challenges associated with proposed § 234.3(a)(17)(viii)?

[33] Scenarios-based testing allows a designated FMU to address an appropriately broad scope of scenarios, including simulation of extreme but plausible events, and should be designed to challenge the assumptions of response, resumption, and recovery practices, including governance arrangements and communication plans.

10. Is the proposed formulation of "two sites providing for sufficient redundancy supporting critical operations" a clear and appropriate replacement for references to "primary" and "secondary" sites in the current rule?
11. Is the proposed requirement on addressing "reconnection" of the designated FMU after a disruption clear? Should a different term be used, given the intention of this proposed requirement, as explained in section II.C.3 above?

D. Third-party risk management

The Board expects a designated FMU to conduct its activities—whether conducted directly by the designated FMU or through a service provider—in a safe and sound manner. The Board is proposing to add § 234.3(a)(17)(ix) regarding the management of risks associated with third-party relationships. Proposed § 234.3(a)(17)(ix) would require a designated FMU to have systems, policies, procedures, and controls in order to effectively identify, monitor, and manage risks associated with third-party relationships. Additionally, for any service that is performed for the designated FMU by a third party, these systems, policies, procedures, and controls would need to ensure that risks are identified, monitored, and managed to the same extent as if the designated FMU were performing the service itself. Importantly, the risks associated with third-party relationships would include both the risks stemming from the third party itself, as well as risks stemming from the supply chain.

Additionally, the Board is proposing to add "third party" as a defined term in Regulation HH. Specifically, proposed § 234.2(n) would define "third party" as "any entity with which a designated FMU maintains a business arrangement, by contract or otherwise."[34] For the purposes of proposed § 234.3(a)(17)(ix), the Board would consider third-party relationships to include

[34] Participants of designated FMUs would not be considered third parties. This definition is consistent with the definition of "third-party relationship" in the proposed interagency guidance on third-party relationships. *See* 86 FR 38182, 38186–87 (July 17, 2021). The Board views the requirements of proposed § 234.3(a)(17)(ix) as broadly consistent with the proposed interagency guidance. In examining designated FMUs under Regulation HH, Board examiners will continue to reference guidance on third-party risk management.

vendor relationships for products such as for software and arrangements for any services that third parties perform for a designated FMU.[35] Services can include a wide variety of arrangements, from HVAC services that support the physical infrastructure of the designated FMU to technology platforms or financial risk management modeling that are essential to executing the designated FMU's payment, clearing, or settlement activities. The Board believes that where a designated FMU outsources the provision of services to a third party, the designated FMU retains the responsibility for meeting the risk-management standards in Regulation HH.

The Board is proposing these requirements because of the importance of ensuring that a designated FMU's activities do not become less safe when they are outsourced to third parties, and because of the importance of managing particular sources of operational risk associated with third-party relationships, including "supply chain risk."[36] Supply chain risk encompasses the potential for harm or compromise to a designated FMU that arises as a result of security risks from its third parties' subcontractors or suppliers, as well as the subcontractors' or suppliers' supply chains, and their products or services (including software that may be used by the third party or the designated FMU).[37]

Further, proposed § 234.3(a)(17)(ix) would require a designated FMU to regularly conduct risk assessments of its third-party relationships and establish, as appropriate, information-sharing arrangements with third parties. Proposed § 234.3(a)(17)(ix) would also require a designated FMU to include third parties in business continuity management and testing,

---

[35] Relatedly, the Board believes this proposal is consistent with section 807(b) of the Dodd-Frank Act, which provides each Supervisory Agency of a designated FMU with authority examine the provision of any service integral to the operation of the designated FMU for compliance with applicable law, rules, orders, and standards to the same extent as if the designated FMU were performing the service on its own premises. 12 U.S.C. 5466(b).

[36] The Board identified supply chain risk as a threat on which the Board is focused in its report on cybersecurity and financial system resilience. *See* Board of Governors of the Federal Reserve System, *Report to Congress: Cybersecurity and Financial System Resilience Report* (September 2021), https://www.federalreserve.gov/publications/files/cybersecurity-report-202109.pdf.

[37] This definition is consistent with NIST's definition of "supply chain risk" in the NIST computer-security incident handling guide. *See* NIST, *Computer Security Incident Handling Guide* (Special Publication 800-61, rev. 2), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

as appropriate. The Board believes these specific measures are critical to a designated FMU's ability to effectively manage risks related to third-party relationships.

In general, the Board would expect a designated FMU to take a rigorous approach to identifying, monitoring, and managing risks associated with third-party relationships. To identify and assess the risks from third parties effectively, it would be prudent for the designated FMU to understand *ex ante* any risks associated with the third party, including details on the services or products the third party will provide and the security controls that the third party has in place. Before entering into a third-party relationship, the designated FMU should have a plan in place to address how it will effectively identify, monitor, and manage the relationship and its associated risks, in order to ensure that the designated FMU can continue to meet the risk-management requirements in Regulation HH. A designated FMU should conduct appropriate due diligence on third parties and should include, as appropriate, provisions in service contracts that establish information-sharing agreements based on the risk level of the third party. Information-sharing arrangements should include, where necessary, expectations related to when the designated FMU would be notified of material operational incidents at the third party.

To assess risk levels of third parties and monitor any changes in these risk levels that may affect a designated FMU and its ecosystem, the designated FMU should ensure that it regularly conducts risk assessments of its third-party relationships and that its information-sharing agreements include, where appropriate, information on the third party's information security controls and operational resilience objectives and capabilities. To manage risks posed by third parties, a designated FMU should adopt risk management practices that are commensurate with the level of risk posed by its third-party relationships, as identified through the risk assessments it conducts. For example, to manage supply chain risks, a designated FMU might require, in its contracts with certain third parties that are critical to its operations and services, mandatory approval from the designated FMU before the service provider may outsource any material elements of its service to another party.

In addition, a designated FMU should include third parties in its business continuity management and testing, as appropriate. A designated FMU should run scenario exercises with third parties to ensure that the designated FMU can effectively manage any instances in which a third party experiences an incident causing disruption or material degradation to the designated FMU's critical operations or services. For example, a designated FMU should be prepared to react—such as by switching to a contingency plan—to a cyberattack on one of its third parties that causes disruptions in that entity's ability to enable the designated FMU to fulfill its obligations on time.

1. *Questions*

With respect to proposed § 234.3(a)(17)(ix), the Board requests comment on the following specific questions:

12. Are there other risk-management measures that are essential to effective management of third-party relationship risks that the Board should consider setting as an explicit minimum requirement?
13. Is the proposed requirement on managing risks associated with "third-party" relationships clear? Should a different term be used, given the intention of this proposed requirement, as explained in section II.D above?
14. Are there challenges associated with implementation of this proposed requirement that the Board has not considered?
15. Should the proposed requirements related to third-party risk management be codified in § 234.3(a)(17) as proposed, or should the Board consider an alternative placement for these requirements in Regulation HH?

E. Technical revisions

1. Definition of operational risk

Proposed § 234.2(h) would add "operational risk" as a defined term in Regulation HH. Under the proposal, this term is defined as "the risk that deficiencies in information systems or

internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided by the designated financial market utility."

The proposed definition of "operational risk" is consistent with the definition for operational risk in the PFMI and the Board's definition in part I of the *Federal Reserve Policy on Payment System Risk* (PSR policy), which sets out the Board's views, and related standards, regarding the management of risks in financial market infrastructures, including those operated by the Reserve Banks.[38] The Board also provided this definition of operational risk when it proposed the current operational risk-management standard in Regulation HH in 2014; however, the Board did not believe a defined term in the rule text was necessary at that time. For clarifying purposes, the Board is proposing to adopt "operational risk" as a defined term.

2. Definition of critical operations and critical services

Proposed § 234.2(d) would add "critical operations" and "critical services" as defined terms in Regulation HH, in order to streamline references to these terms. Under the proposal, these terms are defined as "any operations or services that the designated financial market utility identifies under 12 CFR 234.3(a)(3)(iii)(A)." Under § 234.3(a)(3)(iii)(A), a designated FMU must identify its critical operations and services related to payment, clearing, and settlement for purposes of developing its integrated plans for recovery and orderly wind-down.

The Board's proposed amendments to § 234.3(a)(17) related to review and testing, incident management and planning, and business continuity management planning, refer to a designated FMU's critical operations and/or services in multiple places. Amending Regulation HH to include definitions of "critical operations" and "critical services" would clarify that the critical operations or services that the designated FMU should consider under paragraph (a)(17) are the same set of critical operations and services that the designated FMU has identified under

[38] The Board revised concurrently the risk-management standards in Regulation HH and part I of the PSR policy based on the PFMI in 2014.

paragraph (a)(3). These technical revisions are not expected to result in changes to designated FMUs' business continuity management and planning.

3. Cross-reference to "other entities" identified in § 234.3(a)(3) on comprehensive management of risk

Current § 234.3(a)(17)(ii) requires a designated FMU to identify, manage, and monitor the risks that its operations might pose to other "financial market utilities and trade repositories, if any." The Board proposes to streamline and replace this reference with other "relevant entities such as those referenced in paragraph (a)(3)(ii)." The Board believes this requirement is consistent with the current requirement under subparagraph (a)(3)(ii) for the designated FMU to identify, measure, monitor, and manage the material risks that it poses to other entities, such as other FMUs, settlement banks, liquidity providers, and service providers, as a result of interdependencies. As a conforming revision, the Board is proposing to include "trade repositories" in the list of entities listed under paragraph (a)(3)(ii).[39]

4. Operational capabilities to ensure high degree of security and operational reliability

Current § 234.3(a)(17)(iii) requires a designated FMU to have "policies and systems" that are designed to achieve clearly defined objectives to ensure a high degree of security and operational reliability. The Board expects a designated FMU to establish clearly defined objectives to ensure a high degree of security and operational reliability; to have systems designed to achieve these objectives; and to have policies, such as benchmarks, in place for the designated FMU to evaluate its systems' performance against these objectives.

A designated FMU is implicitly required to have the operational capability to achieve these objectives. The Board is proposing to make this requirement explicit by clarifying that a designated FMU must have "operational capabilities"—in addition to policies and systems—that are designed to achieve clearly defined objectives to ensure a high degree of security and

[39] Because of the differences in the definition for financial market infrastructure in the PFMI, which includes trade repositories, and the definition of FMU in the Dodd-Frank Act, which does not, the Board inadvertently excluded the reference to "trade repositories" in § 234.3(a)(3)(ii).

operational reliability. This additional emphasis on having operational capabilities in addition to policies and systems is in line with proposed § 234.3(a)(17)(i)(A)(2), which emphasizes the need for a designated FMU to assess whether its relevant systems, policies, procedures, and controls *function as intended*.

5. Identify, monitor, and manage potential and evolving vulnerabilities and threats

Current § 234.3(a)(17)(v) requires a designated FMU to have comprehensive physical, information, and cyber security policies, procedures, and controls "that address" potential and evolving vulnerabilities and threats. The Board is proposing to replace the quoted text with "that enable the designated financial market utility to identify, monitor, and manage" potential and evolving vulnerabilities and threats. The Board believes this is a technical change that would clarify what it means to "address" potential and evolving vulnerabilities and threats.

6. Questions

With respect to the proposed set of technical amendments, the Board requests comment on the following specific question:

16. Would any of these proposed amendments effect a substantive change? If so, how?

III. Administrative Law Matters

A. Regulatory Flexibility Act Analysis

The Regulatory Flexibility Act, 5 U.S.C. 601 *et seq.* (RFA), requires an agency to consider the impact of its proposed rules on small entities. In connection with a proposed rule, the RFA generally requires an agency to prepare an Initial Regulatory Flexibility Analysis (IRFA) describing the impact of the rule on small entities, unless the head of the agency certifies that the proposed rule will not have a significant economic impact on a substantial number of small entities and publishes such certification along with a statement providing the factual basis for such certification in the *Federal Register*. An IRFA must contain (1) a description of the reasons why action by the agency is being considered; (2) a succinct statement of the objectives

of, and legal basis for, the proposed rule; (3) a description of, and, where feasible, an estimate of the number of small entities to which the proposed rule will apply; (4) a description of the projected reporting, recordkeeping, and other compliance requirements of the proposed rule, including an estimate of the classes of small entities that will be subject to the requirement and the type of professional skills necessary for preparation of the report or record; (5) an identification, to the extent practicable, of all relevant Federal rules that may duplicate, overlap with, or conflict with the proposed rule; and (6) a description of any significant alternatives to the proposed rule that accomplish its stated objectives.

The Board is providing an IRFA with respect to the proposed rule. For the reasons described below, the Board believes that the proposal will not have a significant economic impact on a substantial number of small entities. The Board invites public comment on all aspects of its IRFA.

1. Reasons action is being considered

The Board is proposing to amend Regulation HH to update current standards related to operational risk management in light of developments in the operational risk, technology, and regulatory landscape in which designated FMUs operate. Further discussion of the rationale for the proposal is provided in section I.C, above.

2. Objectives of the proposed rule

As described in section I.B, above, section 805(a)(1)(A) of the Dodd-Frank Act requires the Board to prescribe risk-management standards, taking into consideration relevant international standards and existing prudential requirements, applicable to certain designated FMUs. Pursuant to this authority, the Board issued Regulation HH in 2012 and significantly revised Regulation HH in 2014. The Board is now proposing revisions to the current Regulation HH standards related to operational risk management. The Board's objective is to promote effective operational risk management practices at and the operational resilience of designated

FMUs subject to Regulation HH, and as a result, advance safety and soundness and promote the stability of the U.S. financial system.

3. Description and estimate of the number of small entities

Regulation HH applies to designated FMUs other than derivatives clearing organizations registered with the CFTC and clearing agencies registered with the SEC. At present, the FSOC has designated eight FMUs as systemically important; two of these designated FMUs are subject to the Board's Regulation HH.

The Small Business Administration (SBA) has adopted size standards for determining whether a particular entity is considered a "small entity" for purposes of the RFA. The Board believes that the most appropriate SBA size standard to apply in determining whether a designated FMU is a small entity is the SBA size standard for financial transactions processing, reserve, and clearinghouse activities; under this standard, a designated FMU is considered a small entity if its annual receipts are less than $41.5 million.[40] When applying this SBA size standard, the Board includes the assets of all domestic and foreign affiliates in determining whether to classify a designated FMU as a small entity.[41]

After applying this SBA size standard, the Board believes that neither of the designated FMUs that are subject to Regulation HH are considered small entities.

4. Estimating compliance requirements

The proposal updates current standards in Regulation HH related to operational risk management in light of developments in the operational risk, technology, and regulatory landscape in which designated FMUs operate. The proposed revisions are discussed in detail in section II, above. In general, the proposed revisions would add specificity to the current

---

[40] 13 CFR 121.201 (subsector 522320). Alternatively, the SBA size standards for (1) securities and commodities exchanges, (2) trust, fiduciary, and custody activities, or (3) international trade financing activities could also apply to certain designated FMUs; these size standards are currently the same as the size standard for financial transactions processing, reserve, and clearinghouse activities (i.e., annual receipts of less than $41.5 million). *Id.* (subsectors 523210, 523991, and 522293).

[41] 13 CFR 121.103.

operational risk management standards by codifying existing practices of designated FMUs into the regulation. Because the proposed revisions do not represent a significant change from existing practices of designated FMUs, the Board would not expect the proposed revisions to have a significant economic impact on those small entities.

5. Duplicative, overlapping, and conflicting rules

The Board is not aware of any federal rules that may duplicate, overlap with, or conflict with the proposed rule.

6. Significant alternatives considered

The Board did not consider any significant alternatives to the proposed rule. The Board believes that updating the current Regulation HH standards related to operational risk management in light of developments in the operational risk, technology, and regulatory landscape in which designated FMUs operate is the best way to achieve the Board's objectives of promoting effective operational risk management practices at and the operational resilience of designated FMUs subject to Regulation HH, and as a result, advancing safety and soundness and promoting the stability of the U.S. financial system.

B. Competitive Impact Analysis

As a matter of policy, the Board conducts a competitive impact analysis in connection with any operational or legal changes that could have a substantial effect on payment system participants, even if competitive effects are not apparent on the face of the proposal. Pursuant to this policy, the Board assesses whether proposed changes "would have a direct and material adverse effect on the ability of other service providers to compete effectively with the Federal Reserve in providing similar services" and whether any such adverse effect "was due to legal differences or due to a dominant market position deriving from such legal differences." If, as a result of this analysis, the Board identifies an adverse effect on competition, the Board then

assesses whether the associated benefits – such as improvements to payment system efficiency or integrity – can be achieved while minimizing the adverse effect on competition.[42]

Designated FMUs are subject to the supervisory framework established under Title VIII of the Dodd-Frank Act. This proposed rule revises current Regulation HH operational risk-management standards for certain designated FMUs. At least one designated FMU that is currently subject to Regulation HH competes with a similar service provided by the Reserve Banks.

Under the Federal Reserve Act, the Board has general supervisory authority over the Reserve Banks, including the Reserve Banks' provision of payment and settlement services. This general supervisory authority is more extensive in scope than the Board's authority over certain designated FMUs under Title VIII. In practice, Board oversight of the Reserve Banks goes beyond the typical supervisory framework for private-sector entities, including the framework provided by Title VIII. The Board is committed to applying risk-management standards to the Reserve Banks' Fedwire Funds Service and Fedwire Securities Service (collectively, Fedwire Services) that are at least as stringent as the Regulation HH standards that are applied to designated FMUs that provide similar services. This would continue to be the case if the proposed revisions to the operational risk management standards in Regulation HH are adopted. Specifically, the Fedwire Services are subject to in the risk-management standards in part I of the PSR policy, which (like those in Regulation HH) are based on the PFMI. The Board is be guided by its interpretation of the corresponding provisions of Regulation HH in its application of the risk management expectations in the PSR policy.[43] Therefore, the Board does not believe the proposed rule will have any direct and material adverse effect on the ability of other service providers to compete with the Reserve Banks.

---

[42] *See Policies: The Federal Reserve in the Payments System* (issued 1984; revised 1990 and January 2001), https://www.federalreserve.gov/paymentsystems/pfs_frpaysys.htm.

[43] *See* section I.B.1 of the PSR policy.

C. Paperwork Reduction Act Analysis

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3506; 5 CFR part 1320, Appendix A.1), the Board reviewed the proposed rule under the authority delegated to the Board by the Office of Management and Budget. For purposes of calculating burden under the Paperwork Reduction Act, a "collection of information" involves 10 or more respondents. Any collection of information addressed to all or a substantial majority of an industry is presumed to involve 10 or more respondents (5 CFR 1320.3(c), 1320.3(c)(4)(ii)). The Board estimates there are fewer than 10 respondents and these respondents do not represent all or a substantial majority of the participants in payment, clearing, and settlement systems. Therefore, no collections of information under the Paperwork Reduction Act are contained in the proposed rule.

List of Subjects in 12 CFR Part 234

Banks, banking, Credit, Electronic funds transfers, Financial market utilities, Securities.

For the reasons set forth in the preamble, the Board proposes to amend part 234 of chapter II of title 12 of the Code of Federal Regulations, as follows:

PART 234 – DESIGNATED FINANCIAL MARKET UTILITIES (REGULATION HH)

1. The authority citation for part 234 continues to read as follows:

Authority: 12 U.S.C. 5461 *et seq.*

2. Revise § 234.2 as follows:

§ 234.2 Definitions.

(a) ***Backtest*** means the *ex post* comparison of realized outcomes with margin model forecasts to analyze and monitor model performance and overall margin coverage.

(b) ***Central counterparty*** means an entity that interposes itself between counterparties to contracts traded in one or more financial markets, becoming the buyer to every seller and the seller to every buyer.

(c) ***Central securities depository*** means an entity that provides securities accounts and central safekeeping services.

(d) ***Critical operations*** and ***critical services*** refer to any operations or services that the designated financial market utility identifies under 12 CFR 234.3(a)(3)(iii)(A).

(e) ***Designated financial market utility*** means a financial market utility that is currently designated by the Financial Stability Oversight Council under section 804 of the Dodd-Frank Act (12 U.S.C. 5463).

(f) ***Financial market utility*** has the same meaning as the term is defined in section 803(6) of the Dodd-Frank Act (12 U.S.C. 5462(6)).

(g) ***Link*** means, for purposes of § 234.3(a)(20), a set of contractual and operational arrangements between two or more central counterparties, central securities depositories, or securities settlement systems, or between one or more of these financial market utilities and one or more trade repositories, that connect them directly or indirectly, such as for the purposes of participating in settlement, cross margining, or expanding their services to additional instruments and participants.

(h) ***Operational risk*** means the risk that deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided by the designated financial market utility.

(i) ***Orderly wind-down*** means the actions of a designated financial market utility to effect the permanent cessation, sale, or transfer of one or more of its critical operations or services in a manner that would not increase the risk of significant liquidity or credit problems spreading among financial institutions or markets and thereby threaten the stability of the U.S. financial system.

(j) ***Recovery*** means, for purposes of § 234.3(a)(3) and (15), the actions of a designated financial market utility, consistent with its rules, procedures, and other *ex ante* contractual arrangements, to address any uncovered loss, liquidity shortfall, or capital inadequacy, whether arising from participant default or other causes (such as business, operational, or other structural weaknesses), including actions to replenish any depleted prefunded financial resources and liquidity arrangements, as necessary to maintain the designated financial market utility's viability as a going concern and to continue its provision of critical services.

(k) ***Securities settlement system*** means an entity that enables securities to be transferred and settled by book entry and allows transfers of securities free of or against payment.

(l) ***Stress test*** means the estimation of credit or liquidity exposures that would result from the realization of potential stress scenarios, such as extreme price changes, multiple defaults, and changes in other valuation inputs and assumptions.

(m) ***Supervisory Agency*** has the same meaning as the term is defined in section 803(8) of the Dodd-Frank Act (12 U.S.C. 5462(8)).

(n) ***Third party*** means any entity with which a designated financial market utility maintains a business arrangement, by contract or otherwise.

(o) ***Trade repository*** means an entity that maintains a centralized electronic record of transaction data, such as a swap data repository or a security-based swap data repository.

3. Amend § 234.3 by:

(a) Revising the section heading;

(b) Adding the words “trade repositories,” after the words “such as other financial market utilities,” in paragraph (a)(3)(ii);

(c) Removing the word “following” and adding in its place “after”, in paragraph (a)(3)(iii)(G);

(d) Revising paragraph (a)(17); and

(e) Removing the word “following” and adding in its place “to reflect”, in paragraph (a)(23)(v).

The revisions read as follows:

§ 234.3 Standards for designated financial market utilities.

(a) * * * * *

(17) ***Operational risk.*** The designated financial market utility manages its operational risks by establishing a robust operational risk-management framework that is approved by the board of directors. In this regard, the designated financial market utility -

(i) Identifies the plausible sources of operational risk, both internal and external, and mitigates their impact through the use of appropriate systems, policies, procedures, and controls – including those specific systems, policies, procedures, or controls required pursuant to this paragraph (a)(17) – that are reviewed, audited, and tested periodically and after major changes such that –

(A) The designated financial market utility conducts tests –

(*1*) In accordance with a documented testing framework that addresses scope, frequency, participation, interdependencies, and reporting; and

(*2*) That assess whether the designated financial market utility’s systems, policies, procedures, or controls function as intended;

(B) The designated financial market utility reviews the design, implementation, and testing of systems, policies, procedures, and controls, after material operational incidents,

including the material operational incidents described in paragraph (a)(17)(vi)(A) of this section, or after significant changes to the environment in which the designated financial market utility operates; and

(C) The designated financial market utility remediates as soon as possible, following established governance processes, any deficiencies in systems, policies, procedures, or controls identified in the process of review or testing;

(ii) Identifies, monitors, and manages the risks its operations might pose to other relevant entities such as those referenced in paragraph (a)(3)(ii) of this section;

(iii) Has policies, systems, and operational capabilities that are designed to achieve clearly defined objectives to ensure a high degree of security and operational reliability;

(iv) Has systems that have adequate, scalable capacity to handle increasing stress volumes and achieve the designated financial market utility's service-level objectives;

(v) Has comprehensive physical, information, and cyber security policies, procedures, and controls that enable the designated financial market utility to identify, monitor, and manage potential and evolving vulnerabilities and threats;

(vi) Has a documented framework for incident management that provides for the prompt detection, analysis, and escalation of an incident, appropriate procedures for addressing an incident, and incorporation of lessons learned following an incident. This framework includes a plan for notification and communication of material operational incidents to identified relevant entities that ensures the designated financial market utility –

(A) Immediately notifies the Board when the designated financial market utility activates its business continuity plan or has a reasonable basis to conclude that –

(*1*) There is an actual or likely disruption, or material degradation, to any critical operations or services, or to its ability to fulfill its obligations on time; or

(*2*) There is unauthorized entry, or the potential for unauthorized entry, into the designated financial market utility's computer, network, electronic, technical, automated, or similar systems that affects or has the potential to affect its critical operations or services;

(B) Establishes criteria and processes providing for timely communication and responsible disclosure of material operational incidents to the designated financial market utility's participants and other relevant entities, such that –

(*1*) Affected participants are notified immediately of actual disruptions or material degradation to any critical operations or services, or to the designated financial market utility's ability to fulfill its obligations on time; and

(*2*) All participants and other relevant entities, as identified in the designated financial market utility's plan for notification and communication, are notified in a timely manner of all other material operational incidents that require notification under paragraph (a)(17)(vi)(A) of this section;

(vii) Has business continuity management that provides for rapid recovery and timely resumption of critical operations and services and fulfillment of its obligations, including in the event of a wide-scale disruption or a major disruption;

(viii) Has a business continuity plan that -

(A) Incorporates the use of two sites providing for sufficient redundancy supporting critical operations that are located at a sufficient geographical distance from each other to have a distinct risk profile;

(B) Is designed to enable critical systems, including information technology systems, to recover and resume critical operations and services no later than two hours following disruptive events;

(C) Is designed to enable it to complete settlement by the end of the day of the disruption, even in case of extreme circumstances;

(D) Sets out criteria and processes that address the reconnection of the designated financial market utility to participants and other entities following a disruption to the designated financial market utility's critical operations or services;

(E) Provides for testing, pursuant to the requirements under paragraphs (a)(17)(i)(A) and (a)(17)(i)(C) of this section, at least annually, of the designated financial market utility's business continuity arrangements, including the people, processes, and technologies of the sites required under paragraph (a)(17)(viii)(A), such that it can demonstrate that –

(*1*) The designated financial market utility can run live production at the sites required under paragraph (a)(17)(viii)(A);

(*2*) The designated financial market utility's solutions for data recovery and data reconciliation enable it to meet its recovery and resumption objectives even in case of extreme circumstances, including in the event of data loss or data corruption; and

(*3*) The designated financial market utility has geographically dispersed staff who can effectively run the operations and manage the business of the designated financial market utility; and

(F) Is reviewed, pursuant to the requirements under paragraphs (a)(17)(i)(B) and (a)(17(i)(C) of this section, at least annually, in order to –

(*1*) Incorporate lessons learned from actual and averted disruptions; and

(*2*) Update scenarios and assumptions in order to ensure responsiveness to the evolving risk environment and incorporate new and evolving sources of operational risk; and

(ix) Has systems, policies, procedures, and controls that effectively identify, monitor, and manage risks associated with third-party relationships, and that ensure that, for any service that is performed for the designated financial market utility by a third party, risks are identified, monitored, and managed to the same extent as if the designated financial market utility were performing the service itself. In this regard, the designated financial market utility –

(A) Regularly conducts risk assessments of third parties and establishes information-sharing arrangements, as appropriate, with third parties; and

(B) Includes third parties in business continuity management and testing, as appropriate.

* * * * *

By order of the Board of Governors of the Federal Reserve System.

Margaret McCloskey Shanks,
Deputy Secretary of the Board.

[FR Doc. 2022-21222 Filed: 10/4/2022 8:45 am; Publication Date: 10/5/2022]